Privacy Impact Assessment (PIA): FDA - COMSTAT - QTR1 - 2024 - FDA2125142

Created Date: 1/10/2024 3:02 PM Last Updated: 3/22/2024 6:17 PM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	FDA - COMSTAT - QTR1 - 2024 - FDA2125142	**PIA ID:**	1754540
Name of Component:	FDA - OII Compliance Status Profile System	**Name of ATO Boundary:**	CBER Office of Regulatory Operations
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	73
Submission Status:	Submitted	**Submit Date:**	3/8/2024
Next Assessment Date:	N/A	**Expiration Date:**	3/22/2027
Office:		**OPDIV:**	FDA
Security Categorization:	Moderate	**OpDiv PIA ID:**	FDA2125142
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	7/6/2022
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	Compliance Status Profile System (COMSTAT) provides a summary of several key quality assurance items of information about domestic and foreign firms that manufacture, repack, label/relabel, sterilize, or test drug, medical device, or biological products. The only PII COMSTAT provides are Firm profiles information indicating a firm's compliance status with Current Good Manufacturing Practice (CGMP) or Quality Systems regulations as well as Firm Name and Address information. These Firms may use a company point of contact or they might use the name of their company. Users are provided a user interface to search and view this information. COMSTAT is both an internal and external application. If connected to the FDA Virtual Private Network (VPN), any FDA user can access the site. External users must use a username and password to access the application.

PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	Compliance Status Profile System COMSTAT accesses information about domestic and foreign firms that manufacture, repack, label/relabel, sterilize, or test drug, medical device, or biological products. The system component provides Firm profiles information indicating a firm's compliance status with Current Good Manufacturing Practice (CGMP) or Quality Systems regulations as well as PII such as the Firm Name and Address information. The data that COMSTAT accesses from FACTS database will only relate to PII if the firm/vendor entity name includes the name of an individual (e.g., Tom Smith Training Services, Inc). The fields that it accesses are stored in the FACTS database, and it maintains this data for a minimum of what is defined in the National Archives and Records Administration (NARA) guidelines. COMSTAT does access PII.
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Username Password
PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	Compliance Status Profile System (COMSTAT) allows users to search through a summary of several key quality assurance items of information about domestic and foreign firms that manufacture, repack, label/relabel, sterilize, or test drug, medical device, or biological products. COMSTAT provides Firm profiles information indicating a firm's compliance status with Current Good Manufacturing Practice (CGMP) or Quality Systems regulations as well as Firm Name and Address information. COMSTAT is used by any FDA employee needing to gather information on specific Firms for any compliance, inspections or recall related activities. Users are provided a user interface to search and view this information. COMSTAT is both an internal and external application. If connected to the FDA Virtual Private Network (VPN), any FDA user can access the site. External users must use a username and password to access the application.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	Yes

PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	COMSTAT's website provides a summary of several key quality assurance items of information about domestic and foreign firms that manufacture, repack, label/relabel, sterilize, or test drug, medical device, or biological products. There are two versions of the application. One version is hosted on the FDA intranet and accessible by FDA network users. Another version is accessible by account holders over the internet. Provide Firm profiles information indicating a firm's compliance status with Current Good Manufacturing Practice (CGMP) or Quality Systems regulations as well as Firm Name and Address information. Users are provided a user interface to search and view this information. COMSTAT is both an internal and external application. If connected to the FDA VPN, any FDA user can access the site. External users must use a username and password to access the application. URL: Intranet version: http://intranetapps.fda.gov/scripts/mpqa/index.cfm Internet version: https://www.accessdata.fda.gov/scripts/ora/mpqa/security.cfm
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	

PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Mailing Address User Credentials Other - Free text Field - If firm/vendor entity name includes the name of an individual (e.g., Tom Smith Training Services, Inc) typically non-PII information about the business may in that rare case be PII: (a) firm/vendor (individuals') name; (b) account number with firm/vendor; (c) firm/vendor mailing address and phone; (d) firm/vendor contact Name; (e) firm/vendor email and; (f) firm/vendor website.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	201 - 500
PIA - 4:	For what primary purpose is the PII used?	PII is used to track accounts for FDA users including first and last name and role within the system. Firm/Vendors and their POC including name, email, firm/vendor address, POC email/phone number and the account number with the firm/vendor are stored to track firm/vendors as well as purchases made from the firm/vendor.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The FDA makes no secondary use of the PII.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 374; Public Health Service Act, 42 U.S.C. 262-264; 5 U.S.C. 301.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No

PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Hard Copy Mail/Fax Email Online Government Sources Within the OPDIV Non-Government Sources Members of the Public Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	COMSTAT does not collect any information on the public and therefore, does not require an OMB information collection approval number.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	FDA personnel cannot opt out of the collection of the PII; it is necessary for account use and authentication. Firms/Firm/Vendors must have PII (e.g., point of contact information) submitted if it is allowed to do business in the United States. Firm/Vendors may opt out by providing organizational non-PII contact information such as organizational contact data as appropriate.

PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	If FDA practices change regarding the collection or use of PII for the FDA's Systems for Inspections, Recall, Compliance and Enforcement (SIRCE), the agency will provide any required notice and obtain consent from individuals. Notice procedures may include Federal Register notices, hard copy mail to individuals, adding or updating online notices and disclaimers, or using other available technological means for notification and consent.
PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	Individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any FDA system have multiple options available for assistance. External individuals (firm/vendor personnel) may contact the FDA organization that is purchasing their product or service or may contact the FDA's main office using information provided on FDA.gov. The contacted FDA organization would then engage with the appropriate internal resource to address the issue. FDA personnel may access their Enterprise Administrative Support Environment (EASE) data on their own to update or correct their information. Individuals may also contact the FDA's Privacy Office, their Information System Security Officer, or FDA's Employee Resources and Information Center (ERIC) to seek assistance with any PII use or disclosure concerns or to correct inaccurate information. Also, individuals may report concerns to the FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) via email, phone, and standard mail (all listed on the FDA intranet). In the event of a suspected incident or data breach, all FDA personnel and Direct Contractors are required to report that without delay to the FDA's CIOCC and Privacy Office.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	All PII is relevant by design of the system to collect only essential data. For example, point of contact information is necessary to communicate with firm/vendors and employee PII is similarly necessary for contact purposes as well as system administration and purchase tracking. Accuracy is ensured by individual review of purchase orders. System accounts are reviewed on a regularly basis to determine if access is still required for each user. Integrity and availability are protected by privacy-supporting security controls selected and implemented in the course of providing the system with an authority to operate (ATO). Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199.

PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: completing, documenting, reviewing purchases Administrators: Administrators have access to PII in the course of performing analysis of historical activities and to review work in process. Developers: Developers have access to PII to perform level 3 helpdesk support Contractors: Helpdesk consists of Direct Contractors who have access to PII to perform level 1 and 2 helpdesk support activities.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	System access requests are reviewed and approved by the system/business owner along with the SIRCE (parent system) management team. System accounts are reviewed on a regularly basis to determine if access is still required for each user. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access).
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	Supervisors indicate when accounts are created to apply the minimum information system access that is required for the user to complete his/her job. The access list for the information system is reviewed on a quarterly basis and users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system. System settings, network-level controls (SSO) and access credentials are applied as technical means to limit access to need-to-know at the individual level.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.	All FDA personnel complete mandatory security and privacy awareness training at a minimum of once a year.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users receive system-specific training, review and adhere to the Rules of Behavior, and may obtain additional privacy guidance from the agency's privacy officials.

PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The records handled in COMSTAT are governed by a variety of records schedules specific to the nature of the records. The retention and destruction periods generally range from 10 to 30 years after an action closes or when a record is no longer needed. COMSTAT database records are maintained in accordance with National Archives and Records Administration (NARA) approved citation N1-088-09-3 which states that records disposition is temporary, with records deleted or destroyed 10 years after the end of the fiscal year in which the subject regulatory action is final. Program management files fall under NARA approved citation N1-88-07-2.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include uses of firewalls; access controls such as usernames and passwords; and regular testing of information technology systems. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	3/8/2024
Privacy Analyst Comments:	Updated: PIA -14 PIA – 15	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Updated per HHS comments.	**SOP Review Date:**	3/8/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	3/11/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte All comments have been addressed, submitting for SAOP review and approval. 1/24/2024 Per FDA's email this PIA is being "Rejected" for updates. All comments have been addressed, this PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	3

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	3/22/2024
		SAOP Days Open:	11

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
(1-23-2024) Email_Compliance Status Profile System, ORA Field Workforce Planning System, ORA ShelfLife.pdf	850926	.pdf	1/24/2024 12:38 PM	0
3-8-2024 RE_ PIAs in Queue (ORA Shelflife, ORA Compliance Status Profile System, ORA Field Workforce Planning System).pdf	356191	.pdf	3/11/2024 10:21 AM	0
ORA Compliance Status Profile System_ SOP Approved.pdf	178412	.pdf	3/11/2024 11:16 AM	0
ORA Compliance Status Profile System_SOP Approved.pdf	237016	.pdf	1/11/2024 3:02 PM	0
ORA Compliance Status Profile System_SOP Approved.pdf	178323	.pdf	2/9/2024 8:14 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 14	VILLAFUERTE, NESTOR	1/11/2024	Please define acronym "RES"	
PIA - 15	VILLAFUERTE, NESTOR	1/11/2024	Please define acronym "EASE"	
PIA - 1	BLAND, CRYSTAL	1/11/2024	On the next iteration of the PTA please update: PTA-4: Spell ORA. PTA-9: Spell out URL.	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	3/22/2024 6:17 PM	**History Log:**	View History Log